UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

| APPLICATION NO. | FILING DATE | FIRST NAMED INVENTOR | ATTORNEY DOCKET NO. | CONFIRMATION NO. |
|---|---|---|---|---|
| 10/524,057 | 12/29/2005 | Tai Pang Chen | 212/688US | 4440 |

23371 7590 06/09/2008
CROCKETT & CROCKETT, P.C.
26020 ACERO
SUITE 200
MISSION VIEJO, CA 92691

| EXAMINER | |
|---|---|
| WRIGHT, BRYAN F | |

| ART UNIT | PAPER NUMBER |
|---|---|
| 2131 | |

| MAIL DATE | DELIVERY MODE |
|---|---|
| 06/09/2008 | PAPER |

**Please find below and/or attached an Office communication concerning this application or proceeding.**

The time period for reply, if any, is set in the attached communication.

| Office Action Summary | Application No. | Applicant(s) | |
|---|---|---|---|
| | 10/524,057 | CHEN ET AL. | |
| | Examiner | Art Unit | |
| | BRYAN WRIGHT | 2131 | |

*-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --*

**Period for Reply**

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE *3* MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

**Status**

1)☒ Responsive to communication(s) filed on *29 December 2005*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

**Disposition of Claims**

4)☒ Claim(s) *1-61* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-61* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

**Application Papers**

9)☐ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *08 February 2005* is/are: a)☒ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

**Priority under 35 U.S.C. § 119**

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

**Attachment(s)**

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☒ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date *5/5/2005, 2/8/2005*.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

## DETAILED ACTION

1. This action in response to application December 29, 2005. Claims (1-61) are pending.

### *Claim Rejections - 35 USC § 102*

The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (b) the invention was patented or described in a printed publication in this or a foreign country or in public use or on sale in this country, more than one year prior to the date of application for patent in the United States.

2. Claims 1-9, 12, and 13 are rejected under 35 U.S.C. 102(b) as being anticipated by Burger (US Patent No. 6,219,439 cited from IDS).

**3.** As to claim 1, Burger teaches a **method of authenticating a user according to a biometrics parameter of the user presented at an authentication device on a user-presented device on which is stored a biometrics identification template** (i.e., fingerprint template) **divided into a secure portion and an open portion, the method comprising:**

**transmitting to a client terminal** (i.e., smart card reader interface) **data derived from said user biometrics parameter at the authentication device** [fig. 2; col. 6, lines 39-51]);

**transmitting from a user-presented device** (i.e., smart card) **to the client terminal only the open portion of the said biometrics identification template** (i.e.,

fingerprint template) **held on the user-presented device** (i.e., smart card) (i.e., Burger teaches performing data transmission based on comparing biometric data captured from user with stored biometric data (e.g., fingerprint template) [fig. 2; col. 6, lines 39-51]);

**at the client terminal** (i.e., smart card reader interface) **implementing a first stage of an identity authentication process between said data and said portion and transmitting the results of said authentication process to the user-presented device** (i.e., smart card) (i.e., Burger teaches a system contain a smart card, smart card reader and PC for which a form of user authentication is performed [col. 6, lines 49-52]);

**and at the user-presented device** (i.e., smart card) **implementing a second stage to complete the identity authentication process using said results and issuing an authentication result based thereon** (i.e., Burger teaches a system comprising a device for which user biometric authentication is performed [col. 6, lines 39-49]).

4. As to claim 2, Burger teaches a **method of registration of a user according to a biometrics parameter of the user presented at an authentication device, the method comprising; transmitting to an authorized client terminal** (i.e., smart card reader interface) **data** (i.e., user identification) **said user biometrics parameter obtained at the authentication device** [fig. 2; col. 6, lines 39-51];

**at the authorized client terminal** (i.e., smart card reader interface), **dividing the biometrics identification template computed into secure portion and open**

**portion, transmitting from the authorized client terminal** (i.e., smart card reader interface) (i.e., Burger teaches a biometric characteristics of a user residing on a portable standalone device [col. 4, lines 1-5] Burger teaches biometric template data used for comparing with said user stored portable standalone biometric characteristics [col. 6, lines 39-52], **to a user-presented device** (i.e., smart card) **both the open portion and the secure portion of a biometrics identification template** (i.e., Burger teaches biometric characteristics residing on a user standalone device [col. 4, lines 1-5], **storing the said template consisting of open and secure portions on the user-presented device** (i.e., Burger teaches storing a biometric authentication data **(**i.e., fingerprint template) on a storage medium device (i.e., smart card) [col. 3, lines 55-60]).

5. As to claim 3, Burger teaches a **method where the secure portion of the biometrics identification template is the portion containing data unauthorized modification of which may cause an impostor to be incorrectly authenticated as a genuine user** (i.e., Burger teaches user biometric characteristics stored on a portable standalone device [fig. 1]).

6. As to claim 4, Burger teaches a **method where the open portion** (i.e., user identification data) **of the biometrics identification template is the portion containing data unauthorized modification of which may not cause an impostor to be incorrectly authenticated as a genuine user** (i.e., Burger teaches user

identification data transmittal upon user biometric characteristic validated [col. 7, lines 1-5]).

**7.** As to claim 5, Burger teaches a **method where the biometrics parameter is a Fingerprint** (col. 6, lines 14-16).

8. As to claim 6, Burger teaches a **method said open portion of the template comprises parameters** (i.e., encrypted user identification information) **of a predetermined number of unique features of the Template** (i.e., Burger teaches encrypted user identification information associated with user biometric characteristic stored on a portable standalone device validated [col. 7, lines 1-5]).

**9.** As to claim 7, Burger teaches a **method where the first stage of said identity authentication process implemented at the client terminal** (i.e., 12, fig. 2**) comprises locating unique features using the data derived from the user biometrics parameter and aligning them with said predetermined number of unique features from the identification template held on the user-presented device** (i.e., smart card) (i.e., Burger teaches an authentication process where the user inserts a portable standalone device containing user biometric characteristic [12, 14, fig. 2]).

10. As to claim 8, Burger teaches a **method where the second stage of the said identity authentication process implemented on the user-presented device** (i.e., smart card) **is implemented using a local executable matching program** (i.e., application) stored on the device (i.e., Burger teaches the smart card contains a micro computer for application [col. 6, lines 17-20]).

**11.** As to claim 9, Burger teaches a **method where the first stage of the identity authentication process implemented at the client terminal** (i.e., reader) **is implemented using a client executable matching program** (i.e., Burger teaches a system with a reader compares user biometric characteristics [col. 6, lines 14-16]).

12. As to claim 12, Burger teaches a **method where the authentication result is used to authenticate a user for authorizing a secure transaction** (i.e., ATM transaction) (i.e., Burger teaches authenticating user at an ATM [col. 8, lines 15-25].

**13.** As to claim 13, Burger teaches a **method where the secure transaction is controlled by an executable transaction program stored on the user-presented device** (i.e., Burger teaches a smart card used in authentication. Burger further teaches the capability to employ said smart card authentication practice with an ATM transaction [col. 8, lines 15-25]).

14. Claims 38-43, 45-61 are rejected under 35 U.S.C. 102(e) as being anticipated by Studd et al. (US Patent Publication No. 2004/0122774 and Studd hereinafter).

**15.** As to claim 38, Studd teaches a **method of executing an operation using first and second processors, the method comprising:**

**storing in the first processor a first task table containing a plurality of process names** (i.e., mobile device application) **with associated process identifiers, each associated with a process locator** (i.e., Studd teaches a request for a list of mobile device application from mobile to device for which said mobile device application will be stored and executed [par. 51]);

**storing in the second processor a second task table containing said of process names and process identifiers** (i.e., Studd teaches a mobile device containing list mobile device application [par. 51]);

**identifying at the second processor a process to be executed and issuing a request to the first processor to execute said process** (i.e., Studd teaches identifying a mobile application to execute [par. 51 - par. 53]);

**locating said process using the process locator and executing said process at the first processor to generate a result** [par. 51 - par. 53];

**and returning the result to the second processor** [par. 51 - par. 53].

16. As to claim 39, Studd teaches a **method where said process names** (i.e., identifiers) **include object names associated with respective object identifiers** [par. 51, lines 7-10].

**17.** As to claim 40, Studd teaches a **method where each object has associated therewith a plurality of functions** (i.e., mobile device application) **each identified by function names and associated function identifiers in the first and second task tables** (par. 51).

18. As to claim 41, Studd teaches a **method where the process locator identifies** (i.e., identifier) **the starting address of a process in a program memory** (par. 51, lines 7-10).

**19.** As to claim 42, Studd teaches a **method where the second processor has significantly less processing power than the first processor** (par. 29, lines 8-11).

20. As to claim 43, Studd teaches a **method where the second processor is arranged to execute locally processes requiring less processing power than those executed by the first processor** [fig . 5].

**21.** As to claim 45, Studd teaches a **method where there are a plurality of second processors in communication with a single first processor, each second**

**processor holding a respective task table, and the first processor holding a first task table** (i.e., mobile device application**) including all processes identified by the task tables of the second processors** (i.e., Studd teaches a mobile device with a list of mobile device applications [par. 50- par. 53]).

22. As to claim 46, Studd teaches **a method where a client bridge** (i.e., predetermine mechanism) **is connected between the first and second processors, the client bridge** (i.e., predetermine mechanism) **conveying said requests from the second processor to the first processor and returning the results from the first processor to the second processor** (par. 100).

**23.** As to claim 47, Studd teaches **a method where the first processor is a client terminal and the second processor is embedded on a secure portable computing and data storage platform** [404, fig. 4]

24. As to claim 48, Studd teaches **a method where there are a plurality of first processors connected** (i.e., multiple processors) **via a client bridge to one or more second processor and arranged to implement different subsets of the processes in the task table of the second processor** [par. 29, lines 7-11].

**25.** As to claim 49, Studd teaches a **processing system comprising:**

**a first processor in which is stored a first task table containing a plurality of process names and process identifiers, each associated with a process locator** (i.e., Studd teaches a request for a list of mobile device application from mobile to device for which said mobile device application will be stored and executed [par. 51]);

**a second processor in which is stored a second task table containing said process names with associated process identifiers** (i.e., Studd teaches a mobile device containing list mobile device application [par. 51]);

**the second processor including a distributed object execution manager for identifying a process to be executed and issuing a request to the first processor to execute said process** (i.e., Studd teaches identifying a mobile application to execute [par. 51 - par. 53]);

**and the first processor including a client distributed object execution manager for controlling the execution of said processes at the first processor, the results of execution of the processes implemented at the first processor being returned to the second processor** [par. 51 - par. 53].

26. As to claim 50, Studd teaches a **processing system where the first processor includes a client manager** (i.e., input/output controller hub) **for handling communications between the first and second processors** (par. 31).

**27.** As to claim 51, Studd teaches a **system where the first processor includes an**

**execution manager** (i.e., framework application services unit) **for handling the execution of processes** (i.e., mobile device application) [par. 51 - par. 53].

28. As to claim 52, Studd teaches **a system where the first processor comprises a program store for holding said processes, the process locator** (i.e., identifier) **being used to identify the location of said processes in the program store** [par. 51].

29. As to claim 53, Studd teaches a **system where the second processor includes a remote device manager for transmitting said requests to the first processor** [fig. 4].

30. As to claim 54, Studd teaches a **system where the second processor comprises a stack for holding results returned to it from the first processor** (par. 61)

31. As to claim 55, Studd teaches a **system according where the second processor includes a program store for holding said processes** (par. 51).

32. As to claim 56, Studd teaches a **system where the first processor comprises a client terminal** (fig. 4).

**33.** As to claim 57, Studd teaches a **system which comprises a plurality of first processors, the system further comprising a client bridge** (i.e., predetermine mechanism) **for handling communications between the first processors and the second processor** [par. 100].

34. As to claim 58, Studd teaches **a system where each first processor comprises a server** (par. 100, lines 6-9).

35. As to claim 59, Studd teaches **a system where the client bridge includes a network execution manager** (i.e., input/output controller hub) **for transmitting requests from the second processor to the appropriate one of the first processors, based on a processor identifier in the request** [par. 31, lines 1-8].

36. As to claim 60, Studd teaches a **system comprising a plurality of second processors and a client bridge** (i.e., predetermine mechanism) **for connecting said second processors to said first processor** [par. 100, lines 1-9].

**37.** As to claim 61, Studd teaches a **system where the second or each second processor is embedded on a respective portable secure computing and data storage platform such as smart card** [par. 404, fig. 4].

***Claim Rejections - 35 USC § 103***

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

This application currently names joint inventors. In considering patentability of the claims under 35 U.S.C. 103(a), the examiner presumes that the subject matter of the various claims was commonly owned at the time any inventions covered therein were made absent any evidence to the contrary. Applicant is advised of the obligation under 37 CFR 1.56 to point out the inventor and invention dates of each claim that was not commonly owned at the time a later invention was made in order for the examiner to consider the applicability of 35 U.S.C. 103(c) and potential 35 U.S.C. 102(e), (f) or (g) prior art under 35 U.S.C. 103(a).

38. Claims 14-17, and 23 are rejected under 35 U.S.C. 103(a) as being unpatentable over Burger in view of Studd.

39. As to claim 14 - 17, the system disclose by Burger teaches substantial features of the claim invention (discussed above) it fails to disclose:

**A method where when the authentication result indicates an adequate match, a first security access check key is constructed including the authentication result** (claim 14).

**A method where a second security access check key is requested and compared with the first security access key, the result of said comparison being used to enable the executable transaction program if it yields a positive authentication** result (claim 15).

**A method where the second security access check key is issued from a security** server (claim 16).

**A method where the first and second security access check keys each include a unique identification number** (claim 17).

However, these features are well known in the art and would have been an obvious modification of the system disclosed by Burger as introduced by Studd. Studd discloses:

**A method where when the authentication result indicates an adequate match, a first security access check key** (i.e., private key) **is constructed including the authentication result** (claim 14) (to provide security access key [par. 100]).

**A method where a second security access check key is requested and compared with the first security access key** (i.e., predetermined mechanism),

**the result of said comparison being used to enable the executable transaction program if it yields a positive authentication result** (claim 15) (to provide means to establish a trusted relationship [par. 100]).

**A method where the second security access check key** (i.e., private key) **is issued from a security server** (claim 16) (to provide security access key [par. 100]).

**A method where the first and second security access check keys each include a unique identification number** (i.e., predetermine means) (claim 17) (to provide the means to establish a trusted communication relation ship [par. 100]).

Therefore, given the teachings of Studd, a person having ordinary skill in the art at the time of the invention would have recognized the desirability and advantage of modifying Burger by employing the well known features of establishing a trusted communication relationship disclosed above by Studd, for which distributed authentication will be enhanced [col. 4, lines 25-35].

**40.** As to claim 23, Burger teaches a **method where the access is divided into several levels and wherein the level of access granted to a user is dependent on the confidence level of positive identity obtained from the unique identification**

**number** (i.e., Burger teaches a multilevel authentication process [col. 6, lines 39-67].

41. Claims18-20 are rejected under 35 U.S.C. 103(a) as being unpatentable over Burger in view of Scheidt et al. (US Patent Publication No. 2005/0235148 and Scheidt hereinafter).

42. As to claim 18-20, the system disclose by Burger teaches substantial features of the claim invention (discussed above) it fails to disclose:

**A method where the unique identification number contains a number obtained from a mathematical operation on a randomly generated number and the authentication result** (claim 18).

**A method where the randomly generated number changes at each time the number is used** (claim 19).

**A method where the changing random number is tracked by dividing the number into two portions, a first portion to be used as the current random number and a second portion to be used as the next random number** (claim 20).

However, these features are well known in the art and would have been an obvious modification of the system disclosed by Burger as introduced by Scheidt. Scheidt discloses:

> **A method where the unique identification number contains a number obtained from a mathematical operation on a randomly generated number and the authentication result** (claim 18) (to provide the capability to randomly generate a PIN [par. 383]).
>
> **A method where the randomly generated number changes at each time the number is used** (claim 19) (to provide the capability to randomly generate a PIN [par. 383]).
>
> **A method where the changing random number is tracked by dividing the number into two portions, a first portion to be used as the current random number and a second portion to be used as the next random number** (claim 20) (to provide the capability to randomly generate a PIN [par. 383]).

Therefore, given the teachings of Scheidt, a person having ordinary skill in the art at the time of the invention would have recognized the desirability and advantage of modifying Burger by employing the well known features of randomly generating a PIN disclosed above by Scheidt, for which distributed authentication will be enhanced [par. 383].

43. Claims 10, 11, 24-29 are rejected under 35 U.S.C. 103(a) as being unpatentable over Burger in view of Hamid (US Patent No. 7, 274,804).

44. As to claim 10 and 11, the system disclose by Burger teaches substantial features of the claim invention (discussed above) it fails to disclose:

> **A method where the client executable matching program is stored on the user-presented device or the authentication device and is transmitted to the client terminal at the time of authentication** (claim 10).
>
> **A method where the client executable matching program is downloaded by the client terminal from a remote memory at the time of authentication** (claim 11).

However, these features are well known in the art and would have been an obvious modification of the system disclosed by Burger as introduced by Hamid. Hamid discloses:

> **A method where the client executable matching program** (i.e., biometric template data) **is stored on the user-presented device** (i.e., smart card) **or the authentication device and is transmitted** (i.e., surrendered) **to the client terminal at the time of authentication** (claim 10) (to provide stored biometric matching data [col. 4, lines 25-35]).

**A method where the client executable matching program** (i.e., biometric template) **is downloaded** (i.e., surrendered) **by the client terminal from a remote memory** (i.e., smart card) **at the time of authentication** (claim 11) (to provide stored biometric matching data [col. 4, lines 25-35]).

Therefore, given the teachings of Hamid, a person having ordinary skill in the art at the time of the invention would have recognized the desirability and advantage of modifying Burger by employing the well known features of biometric template matching data from smart card disclosed above by Hamid, for which distributed authentication will be enhanced [col. 4, lines 25-35].

**45.** As to claim 24, Burger teaches a **system for authenticating a user according to a biometrics parameter of the user, the system comprising:**

**a user-presented device** (i.e., smart card) **on which is stored a biometrics identification template divided into a secure portion and an open portion, where only said open portion can be transmitted out of the said device** (i.e., Burger teaches a smart card with user biometric data [col. 6, lines 39-44]);

**an authentication device** (i.e., smart card reader interface) **operable to read biometrics data derived from a user, and comprising means for communicating with the user-presented device and a client terminal** (i.e., Burger teaches a smart card reader interface for reading smart card [ col. 8, lines 1-4- 16]);

However Burger does not expressly teach:

**a client terminal arranged to receive the said open portion of the biometrics identification template held on the user-presented device** (i.e., smart card) **and the biometrics data derived from the user, and comprising a client processor operable to implement a first stage of and identity authentication process between said data and said portion and to transmit the results of said identity authentication process to the user-presented device, and where the user-presented device comprises a device processor operable to implement a second stage to complete the identity authentication process using said results and to issue an authentication result based thereon.**

However, these features are well known in the art and would have been an obvious modification of the system disclosed by Burger as introduced by Hamid. Hamid discloses:

**a client terminal arranged to receive the said open portion of the biometrics identification template held on the user-presented device** (i.e., smart card) **and the biometrics data derived from the user, and comprising a client processor operable to implement a first stage of and identity authentication process between said data and said portion and to transmit the results of said identity authentication process to the user-presented device** (to provide a client terminal authentication capability [col.. 6, lines 20- 35])**, and wherein the user-presented**

**device** (i.e., smart card ) **comprises a device processor operable to implement a second stage to complete the identity authentication process using said results and to issue an authentication result based thereon** (to provide a smart card biometric authentication capability [col. 7, lines 60-67])**.**

Therefore, given the teachings of Hamid, a person having ordinary skill in the art at the time of the invention would have recognized the desirability and advantage of modifying Burger by employing the well known features of biometric authentication disclosed above by Hamid, for which distributed authentication will be enhanced [col. 7, lines 60-67].

**46.** As to claim 25, Burger teaches a **system where the secure portion of the biometrics identification template is the portion containing data unauthorized modification of which may cause the system to incorrectly authenticate an impostor as a genuine user** (i.e., Burger teaches user biometric characteristics stored on a portable standalone device [fig. 2]).

47. As to claim 26, Burger teaches a **system where the open portion of the biometrics identification template is the portion containing data unauthorized modification of which may not cause the system to incorrectly authenticate an** (i.e., Burger teaches user identification data transmittal upon user biometric characteristic validated [col. 7, lines 1-5]).

48. As to claim 27, Burger teaches a **system where the biometrics parameter is a fingerprint** (col. 6, lines 14-16), **and where the authentication device includes a fingerprint Sensor** (i.e., scanner) (col. 5, lines 65-67).

49. As to claim 28, the system disclose by Burger teaches substantial features of the claim invention (discussed above) it fails to disclose:

> **A system where said portion of the template comprises parameters of a predetermined number of unique features of the template** (claim 28).

However, these features are well known in the art and would have been an obvious modification of the system disclosed by Burger as introduced by Hamid. Hamid discloses:

> **A system where said portion of the template comprises parameters of a predetermined number of unique features of the template** (claim 28) (to provide a biometric template with unique features [col. 4, lines 25-30]).

Therefore, given the teachings of Hamid, a person having ordinary skill in the art at the time of the invention would have recognized the desirability and advantage of modifying Burger by employing the well known features of unique biometric template data disclosed above by Hamid, for which distributed authentication will be enhanced [col. 4, lines 25-30].

50. As to claim 29, Burger teaches a **system where the user-presented device** (i.e., smart card) **comprises a memory** (i.e., micro chip) **in which is stored a local executable matching program** (i.e., application) **for implementing the second stage of the matching process** [col. 6, lines 17-20].

51. As to claim 30, Burger teaches a **system where the memory on the user-presented device stores a client executable matching program which is transmitted to the client processor to implement the first stage of the matching process** (i.e., Burger teaches a smart card with a micro computer for storing and running applications [col. 6, lines 17-20]).

52. As to claim 31, Burger teaches **a system which comprises a security server connected to the client terminal** [fig. 2].

53. As to claim 32, the system disclose by Burger teaches substantial features of the claim invention (discussed above) it fails to disclose:

> **A system where the security server holds a client executable matching program for implementing the first stage of the matching process** (claim 32).

However, these features are well known in the art and would have been an obvious modification of the system disclosed by Burger as introduced by Hamid. Hamid discloses:

> **A system where the security server** (i.e., host) **holds a client executable matching program for implementing the first stage of the matching process** (claim 32) (to provide a host with a matching program [col. 6, lines 20-35]).

Therefore, given the teachings of Hamid, a person having ordinary skill in the art at the time of the invention would have recognized the desirability and advantage of modifying Burger by employing the well known features of biometric data matching performed by a host disclosed above by Hamid, for which distributed authentication will be enhanced [col. 6, lines 20-35].

54. Claims 21 and 22 are rejected under 35 U.S.C. 103(a) as being unpatentable over Burger in view Studd as applied to claims 17 above, and further in view of Hamid.

55. As to claim 21 and 22, the system disclose by Burger in view Studd teaches substantial features of the claim invention (discussed above) it fails to disclose:

> **A method where the unique identification number contains a number that is remembered by the user** (claim 21).

**A method where more than one authentication methods can be used to obtain the authentication result, each being incorporated into the unique identification number** (claim 22).

However, these features are well known in the art and would have been an obvious modification of the system disclosed by Burger in view Studd as introduced by Hamid. Hamid discloses:

**A method where the unique identification number** (e.g., PIN) **contains a number that is remembered by the user** (claim 21) (to provide PIN capability for distributed authentication [col. 6, lines 9-15]).

**A method where more than one authentication methods can be used to obtain the authentication result** (to provide various authentication method capability [col. 11, lines 20-25]), **each being incorporated into the unique identification number** (claim 22) (to provide PIN capability for distributed authentication [col. 6, lines 9-15]).

Therefore, given the teachings of Hamid, a person having ordinary skill in the art at the time of the invention would have recognized the desirability and advantage of modifying Burger in view Studd by employing the well known features of PIN entry by user disclosed above by Hamid, for which distributed authentication will be enhanced [col. 4, lines 25-35].

56. Claims 33 -37 are rejected under 35 U.S.C. 103(a) as being unpatentable over Burger in view of Hamid as applied to claims 24 and 31 above, and further in view of Studd.

57. As to claim 33 and 34, the system disclose by Burger in view of Hamid teaches substantial features of the claim invention (discussed above) it fails to disclose:

> **A system where the security server holds a security access check key requestable by the client terminal for enabling a transaction** (claim 33).
>
> **A system which comprises a transaction server arranged to implement secure transactions and which is in communication with the client terminal so that the authentication result is usable to authenticate a user for authorising a secure transaction** (claim 34).

However, these features are well known in the art and would have been an obvious modification of the system disclosed by Burger in view of Hamid as introduced by Studd. Studd discloses:

> **A system where the security server holds a security access check key requestable by the client terminal for enabling a transaction** (claim 33) (to provide access key capability [par. 100, lines 4-7]).

**A system which comprises a transaction server arranged to implement secure transactions and which is in communication with the client terminal so that the authentication result is usable to authenticate a user for authorising a secure transaction** (claim 34) (to provide secure communication capability [par. 100, lines 1-3]).

Therefore, given the teachings of Studd, a person having ordinary skill in the art at the time of the invention would have recognized the desirability and advantage of modifying Burger in view of Hamid by employing the well known features of secure communication disclosed above by Studd, for which distributed authentication will be enhanced [par. 100, lines 1-3].

58. As to claim 35, Burger teaches a **system where the user-presented device stores an executable transaction program** (i.e., biometric data) **for controlling the secure transaction** (i.e., Burger teaches a smart card used in authentication. Burger further teaches the capability to employ said smart card authentication practice with an ATM transaction [col. 8, lines 15-25]).

**59.** As to claim 36, Burger teaches a **system where more than one authentication methods can be used to obtain the authentication result** (i.e., fingerprint and user information authentication [col. 6, lines 39 -67; col. 7, lines 1-6]).

60. As to claim 37, Burger teaches a **system where the access to the transaction server is divided into several levels and wherein the level of access granted to a user is dependent on the confidence level of positive identity obtained based on the results from the various authentication methods used** (i.e., Burger teaches a multi-level authentication process [col. 6, lines 39-67]).

61. Claim 44 is rejected under 35 U.S.C. 103(a) as being unpatentable over Studd in view of Hamid.

62. As to claim 44, the system disclose by Studd teaches substantial features of the claim invention (discussed above) it fails to disclose:

> **A method where the operation being executed is a fingerprint-matching algorithm comprising a base minutiae finding process executed by the first processor and a minutiae matching process executed by the second processor** (claim 44).

However, these features are well known in the art and would have been an obvious modification of the system disclosed by Studd as introduced by Hamid. Hamid discloses:

> **A method where the operation being executed is a fingerprint-matching algorithm comprising a base minutiae finding process executed by the first**

**processor and a minutiae matching process executed by the second processor** (claim 44) (to provide a fingerprint minutiae matching algorithm [col. 7, lines 20-51]).

Therefore, given the teachings of Hamid, a person having ordinary skill in the art at the time of the invention would have recognized the desirability and advantage of modifying Studd by employing the well known features of a fingerprint matching algorithm disclosed above by Hamid, for which distributed authentication will be enhanced [col. 7, lines 20-51].

## Contact Information

Any inquiry concerning this communication or earlier communications from the examiner should be directed to BRYAN WRIGHT whose telephone number is (571)270-3826. The examiner can normally be reached on 8:30 am - 5:30 pm Monday -Friday.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, AYAZ Sheikh can be reached on (571)272-3795. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

**/BRYAN WRIGHT/**
**Examiner, Art Unit 2131**
/Ayaz R. Sheikh/

Supervisory Patent Examiner, Art Unit 2131